5 FAM 890
DIGITALLY SIGNING MACROS

(CT:IM-116; 05-19-2011)
(Office of Origin: IRM/BMP/GRP/GP)

5 FAM 891 POLICY

(CT:IM-116; 05-19-2010)

All macros in applications that have been specified by the Information Integrity Branch of the Systems Integrity Division of the Bureau of Information Resource Management (IRM/OPS/ITI/SI/IIB) will be digitally signed. IRM/OPS/ITI/SI/IIB maintains a list of applications which require macros within the applications to be signed. Macros that are not digitally signed in applications specified by IRM/OPS/ITI/S/IIB will not work. This policy affords no waivers.

5 FAM 892 PROCEDURE

(CT:IM-116; 05-19-2010)

The Department has implemented an online signing application to digitally sign macros. Once the files containing macros are submitted, this tool will digitally sign the macros contained in the file, and return the file to the user. The online application is available via the Public Key Infrastructure (PKI) Signing Utility (PSU). See the *PKI Signing Utility User Instructions* for information about the Public Key Infrastructure (PKI) Signing Utility (PSU).

5 FAM 893 MACRO SECURITY

(CT:IM-116; 05-19-2010)

a. The Department's PKI Program Office (IRM/OPS/ITI/IIB), which has the mission to digitally sign code, is the only office authorized to sign macros. Except for development purposes, the PKI Program Office will not issue certificates for signing macros to other entities within the Department of State. Using the certificates for operational purposes by any other entity in the Department of State is explicitly prohibited.

b. The Department will implement the signing of macros within applications specifically based on known threats.

5 FAM 894 THROUGH 899 UNASSIGNED